UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/716,336	11/18/2003	Nicholas Stamos	3602.1000-003	5223

21005 7590 01/12/2007

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.
530 VIRGINIA ROAD
P.O. BOX 9133
CONCORD, MA 01742-9133

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/716,336	**Applicant(s)** STAMOS ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 November 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *03/05 and 05/05*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This is in reply to application filed on November 18/2003. **Claims 1-22** are pending/examined.

Priority

2. This application is **a continuation of application** 10655573 **which Claims Priority from Provisional application** 60442464, filed on 01/23/2003. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **01/23/2003.**

Drawings

3. Referring to figure 2, on page 7, lines 16-17 of the applicant specification the following has been recited. "The journaling server 104-2 processes atomic event data.and coalesces it into what are **called aggregate events 360**." However, the corresponding drawing figure 2, does not indicate the designated number "360" for aggregate events.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in

the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. <u>**Claims 1-22**</u> are rejected under 35 U.S.C. 102(e) as being anticipated by **Belfiore et al.** (hereinafter referred as **Belfiore**)(U.S. Patent No. 6,990,513 B2) (filed on Jun 22, 2001)

6. <u>**As per claims 1 and 16-17**</u> **Belfiore discloses a system for journaling activity in a data processing system comprising:**

- **A sensor for capturing atomic level events**; *[column 20, lines 57-58, figure 5, ref. Num "606" see "atomic events provided by event sources 602"/As shown on figure 5, ref. Num "606" the atomic events are captured)* *and*

- **An aggregator, for accepting multiple atomic level events and generating a journal event.** *[column 21, lines 4-12] (Event composition 608* ***aggregates,*** *filters, and* ***transforms lower-level events (atomic events 606) which meets the limitation of "multiple atomic level events"*** *into higher-level events 612, which meets the limitation of a journal event. And, at times, maps the events directly into actions, such as world action 614. The actions include real-world actions 614 and information-gathering actions 616 that serve to gather new events via actively polling or listening.* ***Event composition 608 provides methods for combining events*** *and data, whether the events are observed in close temporal proximity or at widely different times)*

7. <u>**As per claims 2-3**</u> **Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein, the journal events are associated with a particular executing process/with a particular user. [column 34-45]** (*The event component 155 of the present invention transparently facilitates the distributed communication of events between any software component that publishes or generates events ("event source") and any software component that*

subscribes to or receives event notifications ("event sink"). In this description and in the claims, an event is an observation about one or more states such as, for example, the status of system components, ***the activity of a user.****)*

8. As per claims 4 and 18 Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system additionally comprising: a filter for filtering atomic level events with an approved event list. *[Column 21, lines 4-19 and column 20, lines 62-column 21, lines 3 and column 22, lines 63-64] (Event composition 608 aggregates, filters, and transforms lower-level events (atomic events 606) into higher-level events 612 and, at times, maps the events directly into actions, such as world action 614. and on column lines it has been disclosed that Event composition may be driven by rules, filters, and by more advanced pattern recognizers spanning a spectrum of sophistication all the way up to rich inferential machinery. Thus, event composition adapts the set of available atomic events 606 into observations 610 that are appropriately matched to* ***the informational requirements of software components/ such requirements meets the limitation of approved event list****, providing them with information at the right level of abstraction to make good decisions.)*

9. **As per claims 5-6 and 19 Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein the approved event list includes a list of approved file identifiers/hash code**.*[Figure 5, ref. Num 610/612 and 622, column 21, lines 3-35] (As shown on figure 5, High level events shown as 612 which meets the limitation of approved event list is stored in event store as shown on figure 5, 622 inferences are performed. Such events should have some kinds of identifier when they are stored and hashing a value for the sake of utilizing the space requirement is something which is also included in storing the list of approved file identifiers / high level events 612)*

10. **<u>As per claims 7 and 20</u> Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system, wherein the sensor is located within a client agent and the aggregator is located within a server.***[Column 21, lines 36-44]*

11. **<u>As per claims 8 and 21</u> Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** additionally comprising: a coalescer for coalescing atomic events output by the sensor prior to inputting them to the aggregator. [Figure 5, ref. Num "606"]

12. **<u>As per claims 9-10 and 22</u> Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system wherein** a bundle of coalesced events is created prior to their transmission between the agent and the server. [Figure 5, ref. Num "608"/event composition meets the limitation of a bundle of coalesced events]

<u>13</u>. **<u>As per claim 11</u> Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein a journal event is detected as a suspect action with a data file. [column 23, lines 64-column 24, lines 22]

14. **<u>As per claim 12</u> Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein an event is attributable to a known user, thread and/or application as identified at a known time. [figure 5, see "Time"]

15. **<u>As per claim 13</u> Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein the coalescer reports an event after a time out period with no activity. *[column 24, lines 21-22, "notify me if there is no mouse movement and no key is pressed in 5 minutes")*

16. **<u>As per claims 14-15</u> Belfiore discloses a system/method as applied to claims above. Furthermore Belfiore discloses the method/system** wherein journal events are used to control security of the data processing system. [column 21, lines 50-53 and column 23, lines 64-column 24, lines 22]

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
01/02/2006

Gilberto B

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100